

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEW JERSEY

ELIZABETH WILBOURNE,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Civil Action No. 13-2149
	)	
EXPERIAN INFORMATION	)	
SOLUTIONS, INC., et al.,	)	
	)	
Defendants.	)	
	)	
	)	

DECLARATION OF KIMBERLY HUGHES  
IN SUPPORT OF DISCOVERY CONFIDENTIALITY ORDER

I, Kimberly Hughes, under penalty of perjury, declare and state as follows:

**I. BACKGROUND**

1. I am employed with Experian Information Solutions, Inc. (hereafter, "Experian") as a Compliance and Litigation Analyst. I have been in that position since January 2011. I have been employed with Experian since 1997. My current duties include the analysis of Experian's credit reporting processes, providing oral and written testimony in connection with litigation against Experian, and review of Experian's policies, procedures and systems as they relate to its consumer reporting business.

2. Based on my experience, I am very knowledgeable about Experian's policies and procedures for the compilation, retention, reinvestigation and disclosure of consumer credit information. I also have reviewed thousands of credit reports, so I have

substantial knowledge about common patterns that occur in the way consumers identify themselves when applying for credit.

3. I submit this declaration in support of the stipulated Discovery Confidentiality Order in the above-captioned matter. The facts set forth herein are based upon my personal knowledge, and if I were called upon to testify to them, I could and would competently do so.

4. Plaintiff seeks to discover certain documents in Experian's possession pertaining to Plaintiff, including: the Administrative Report (the "Admin Report"), the Long Administrative Report (the "long Admin"), the Dispute Response (or "D/R") Log, the Disclosure Request Log, and the Transaction Logs (collectively, the "Confidential Code Documents"). Plaintiff also seeks to discover internal corporate manuals and guidelines containing proprietary information on how Experian maintains its credit reporting procedures (the "Confidential Policy and Procedure Manuals").

## **II. EXPERIAN'S COMPUTER SYSTEM IS ITS BUSINESS**

5. Experian is a national consumer credit reporting agency ("CRA") governed by the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et seq. Experian collects credit information originated by others concerning more than 200 million consumers, such as information about the payment history and balances on a consumer's credit card accounts as well as personal identifying information such as a consumer's name, address, Social Security Number (SSN), and date of birth. Experian provides that information to parties who have been vetted through our stringent membership procedures and who have permissible purpose for credit-related transactions. Experian does not make loans, decide who should receive credit, or set loan terms.

6. Currently, there are three major CRAs in the United States, of which Experian is one. Consumer credit reporting is an extremely competitive business. In most businesses, a computer system is a valuable tool developed to aid management in the running of the business. This is not the case in the credit reporting industry—Experian's computer system *is* its business. As such, Experian has designed a unique and sophisticated computer system to process information received from tens of thousands of diverse lenders and other entities involved in the credit industry, from the public record, and other sources. Experian has spent millions of dollars and countless hours of employee time developing and enhancing its computer system to maximize the accuracy of the credit information it provides to its subscribers. Because of this system and the multitude of processes and procedures Experian has implemented for its use, Experian enjoys a major advantage in the marketplace.

7. Experian diligently guards against the unauthorized or inadvertent disclosure of information relating to its system, including the policies and procedures for its use. To protect its system, Experian has introduced a number of safeguards, including an Information Security Department within Experian, information security regulations, and mandatory information security training of all employees. Experian also restricts access to sensitive documents within its own walls and requires any and all confidential documents in Experian's computers to be encrypted. Such stringent security procedures were developed and implemented at a cost of many millions of dollars.

**III. EXPERIAN'S CONFIDENTIAL CODE DOCUMENTS CONTAIN HIGHLY CONFIDENTIAL AND PROPRIETARY INFORMATION CONCERNING EXPERIAN'S SYSTEM**

8. The Confidential Code Documents contain highly confidential and proprietary trade secrets of Experian which, if disclosed, would pose a risk of severe injury to Experian by revealing closely guarded details about the inner workings of Experian's system.

9. Transaction Logs are used for internal research purposes. They contain coded information, including personal identification numbers, Experian agent identification numbers, and control numbers generated by Experian's system each time a subscriber requests that Experian update, delete, or otherwise change information related to a specific tradeline for reasons other than a consumer's direct dispute with Experian and outside of their normal monthly reporting processes.

10. The Admin Report is a coded document which is specific to a consumer. It is generated by Experian's system and, among other things, contains the name variations, social security numbers, addresses, and credit account information appearing in a consumer's credit files at the time the Admin Report was created. Although the information contained in the Admin Report is kept in the ordinary course of business, the report itself is not created or used in the ordinary course of business.

11. Like the Admin Reports, the Long Admin is specific to the Plaintiff. It includes a coded depiction of both Plaintiff's identifying and credit information as it currently exists in Experian's consumer credit database at the time of the request. Like the Admin Reports, the Long Admin is a coded document that can be generated from Experian's system but does not exist unless Experian makes a special request to compile

information in that format. It is not part of the credit reports provided to third parties, is not part of the file disclosures previously sent to Plaintiff, and although the information contained within the Long Admin is kept in the ordinary course of business, the report itself is not created or generated in the ordinary course of Experian's business.

12. Unlike the Admin Report, however, the Long Admin is rarely used. I find that Long Admins are useful only in an extremely small percentage of cases—e.g., where there is an issue relating to the precise date on which information was reported by a creditor and information relating to the precise date on which account information currently in Experian's files was first loaded onto Experian's system. This case does not fall into that category.

13. D/R Logs summarize dispute activity specific to a consumer. The logs identify the information contained in the report which the consumer disputes, the date of the dispute, the identification numbers of the Experian employee(s) who entered the dispute into Experian's system and who handled the dispute results, the updated information (if any), and the results of the investigation.

14. Disclosure Request Logs summarize the instances in which a consumer's credit file has been accessed. Codes appearing in the Disclosure Request Log include the confidential personal identifying information numbers unique to Plaintiff and the report numbers generated by Experian's computer system when a disclosure was requested.

15. The Confidential Code Documents are all internal Experian reports. They are not part of the credit reports Experian provides to third parties, nor are they part of the file disclosures Experian provides to consumers. They are not created in the normal

course of business, but are generated from Experian's computer systems for a specific consumer and in response to a specific need. These reports may only be generated by a very limited number of trained Experian employees, and access is limited only to those with an absolute need to know.

#### **IV. EXPERIAN FACES RISKS FROM THE DISCLOSURE OF INFORMATION CONCERNING ITS COMPUTER SYSTEM**

16. If, as a result of this litigation, information relating to the design, structure, and inner workings of Experian's computer system (or the policies or procedures used in conjunction with that system) were to be disclosed to unauthorized parties, Experian could be at a great risk of suffering a serious injury to its business and reputation. Experian's ability to compete in the credit reporting industry could be substantially compromised. Third parties that have an incentive to exploit such information include Experian's current and potential competitors, credit clinics, and identity thieves to name a few.

17. *Risk of Reverse-Engineering by Competitors.* The first primary risk is that current or potential competitors could apply reverse-engineering techniques to create or enhance their own systems and remove the competitive edge currently enjoyed by Experian. Information about the structure, logic, and codes of Experian's system would be invaluable to anyone attempting to reverse engineer the system. Experian's competitors and companies hoping to enter the credit reporting industry could build or refine a competing system at a substantially reduced cost and substantially reduced risk. Such competitors would unfairly receive the benefits of Experian's investment and hard work, without having to incur the costs or expend the resources Experian did in developing its system to its current capabilities.

18. Someone seeking to reverse-engineer Experian's system would find the codes, coded information, and other information contained in the confidential documents sought by Plaintiff, as well as the structure of these documents, extremely useful. By comparing the type and nature of information on multiple documents such as these, related to different consumers, a person could undertake to reverse-engineer Experian's system. Each additional document produced and made public would provide more information on the inner workings of Experian's computer system and could therefore provide an incremental benefit to those who would copy Experian's system. As a result, the more examples of these documents that leave Experian, the greater their value becomes to those who would attempt to reverse-engineer Experian's system. Increased access to Experian's confidential documents could therefore increase the probability that outsiders will be able to discern Experian's credit reporting systems and procedures. Accordingly, Experian strives to protect these documents and to avoid producing them without a protective order.

19. *Risks Associated with Credit Clinics.* A second major risk is that unscrupulous credit clinics could use Experian's system information to help their clients avoid the impact of negative, but accurate, credit histories. The documents requested by Plaintiff, such as the Administrative Reports, are coded documents that could reveal details of Experian's sophisticated and highly proprietary matching system, which uses a number of identifiers to link credit information to a particular consumer. If unscrupulous consumers or credit clinics learned the details of that matching system, they could manipulate a consumer's identifying information so as to effectively purge negative credit history or invent inaccurate positive credit information which could boost the consumer's overall

credit rating. As a result, lenders would inadvertently offer loans to unqualified consumers and suffer resulting financial losses. This could lead to massive lending losses for banks and other institutional lenders. These losses would ultimately be passed on to consumers. Such a development would obviously have a profoundly negative impact on Experian's reputation as a provider of reliable information.

20. *Risk of Identity Theft.* The third risk arising from producing these documents without benefit of a protective order is that of identity theft. This information would be of great use to someone seeking to steal another's identity for fraudulent purposes. The information could directly result in identity theft to the extent that Experian is compelled to produce documents revealing the personal information on consumers other than the named Plaintiff. More importantly, the information would indirectly assist identity thieves by educating them on how Experian's system operates and potentially revealing opportunities to subvert it. Armed with such information on the inner workings of Experian's system, identity thieves could victimize millions of consumers. They might also be able to use the information to hide evidence of their crimes from their victims, who often detect identity theft by observing the imposter's activity on their credit reports. Such identity theft typically leads straight into identity fraud, and the hundreds of millions of dollars of losses initially sustained by banks and other lenders are eventually passed onto consumers in the form of higher interest rates, increased fees and higher prices. Over time, the increased risk and incidence of identity theft related to information reported by Experian would also inflict serious harm on Experian's reputation for accuracy and discourage companies from relying on data from Experian.

#### **IV. EXPERIAN FACES RISKS FROM DISCLOSURE OF THE CONFIDENTIAL POLICY AND PROCEDURE MANUALS**



21. The Confidential Policy and Procedure Manuals contain proprietary information on how Experian maintains its credit reporting procedures. The Admin Handbook, for example, explains in detail how to read and interpret every code displayed in the Long Admin. The Admin Handbook contains a listing of the codes that appear in both the Admin Report and the Long Admin. Other materials sought include incentive and salary information demonstrating how Experian's employees' salary and bonus systems operate. Still other manuals walk the reader through Experian's detailed procedures for handling every type of dispute that might arise, including numerous screen shots showing exactly what appears on the computer screen when an Experian employee processes a consumer's dispute.

**A. The Confidentiality of Experian's Policy and Procedure Manuals is Necessary to Protect Experian's Competitive Position in the Credit Reporting Market.**

22. Experian has invested very large sums of money and countless hours of employee time throughout the years developing and enhancing its sophisticated policies and procedures to achieve maximum possible accuracy and completeness of the credit information Experian provides to those with permissible purposes for receiving consumer credit information. By doing so, Experian enjoys a competitive advantage in the credit reporting marketplace.

23. Development of a highly accurate consumer credit reporting system involves delicate incorporation of accumulated knowledge—knowledge which must, therefore, be protected from those who would seek to improve or develop a rival system by obtaining Experian's secrets, instead of investing as extensively as Experian has done over many years and continues to do so today. Heightened protection is necessary for the

incentive and salary information. If these documents were to fall into its competitors' hands, Experian's unique system for promoting and rewarding high-quality and efficient work—a system that provides tangible benefit to Experian and its clients—would be lost.

24. To protect its sensitive information, Experian created numerous safeguards, including an Information Security Department within Experian, information security regulations, and mandatory annual information security training for all employees. Experian also restricts access to sensitive documents within its own walls. In fact, documents containing secret information, such as those presently at issue, are given confidential status at Experian. This is evident by the notation placed on each page of the Confidential Policy and Procedure Manuals at issue stating that the document is "Confidential and Proprietary."

25. Experian's competitors would benefit substantially by gaining access to detailed information regarding Experian's computer software and the confidential, proprietary documentation that reflects the trade secrets of how Experian's computer systems and investigation procedures function. This detailed information is contained in the Confidential Policy and Procedure Manuals at issue.

26. Consequently, if information about its system were to fall into the hands of a current or potential competitor, it would enable the competitor to create or enhance its own procedures and remove the marketing edge currently enjoyed by Experian. Thus, in litigation matters, Experian vigorously strives to ensure that these documents are not produced without a Court-sanctioned protective order.

**B. The Confidentiality of Experian's Policy and Procedure Manuals is Necessary to Protect Consumers.**

27. Furthermore, if the information contained in Experian's Confidential Policy and Procedure Manuals were to fall into criminal hands, it would threaten the credibility of Experian's entire credit reporting system and pose a serious threat to all consumers on which Experian reports information. Such actions could lead to a loss of confidence in Experian's credit reports.

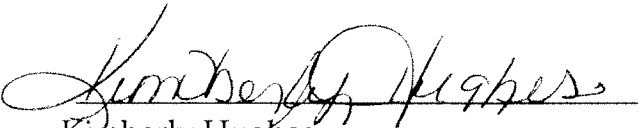
28. More importantly, however, permitting access to Experian's Confidential Policy and Procedure Manuals would open up Experian's system to potential criminals, making it easier for identity theft to take place.

29. For example, Experian's Fraud Procedures Guide shows Experian employees how to delete a security alert or a victim statement at the request of a consumer. Security alerts and victim statements are placed on a consumer's credit file when a consumer believes he or she is at risk for fraudulent activity or after identity theft has already taken place. These alerts serve to protect consumers from future identity theft. By reading Experian's Fraud Procedures Guide, a potential identity thief would know exactly what information Experian needs to delete a security alert or victim statement from a credit file. That identity thief could then fraudulently provide this information to Experian, thus returning an unsuspecting consumer's file to a less-protected status.

30. Disclosure of the Confidential Policy and Procedure Manuals to the public effectively shows potential criminals exactly how Experian's system works, creating a high risk that those individuals would be able to develop methods to successfully circumvent Experian's procedures.

I declare under penalty of perjury that the foregoing is true and correct.

Executed at Allen, Texas, on April 14 2014.

  
Kimberly Hughes